



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/076,952	02/15/2002	Michael P. Lyle	RECOP020	3408
21912	7590	05/09/2006	EXAMINER	
VAN PELT, YI & JAMES LLP 10050 N. FOOTHILL BLVD #200 CUPERTINO, CA 95014			MERED, HABTE	
			ART UNIT	PAPER NUMBER
			2616	

DATE MAILED: 05/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/076,952

Applicant(s)

LYLE, MICHAEL P.

Examiner

Habte Mered

Art Unit

2616

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 February 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The amendment filed on 2/21/2006 has been entered and fully considered.
2. Claims 1-15 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 1-15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin et al (US 6, 578, 147), hereinafter referred to as Shanklin, in view of Hooper et al (US Pub. No. 2003/0067934), hereinafter referred to as Hooper.

Shanklin teaches a multi-processor (i.e. parallel processor) intrusion detector with load balancing for high-speed networks.

Hooper discloses how a router determines to forward a network packet.

5. Regarding **claims 1, 14, and 15**, Shanklin teaches a method and system for routing data packets for network flow analysis by a multi-processor system having a plurality of processors (**See Figure 2 and 3; Sensors 11 make up the multi-processor system**), comprising:

receiving a data packet, the data packet comprising data sufficient to identify a network connection with which the data packet is associated (**See Column 4, Lines 32-40**); and assigning the data to one of the plurality of processors for analysis. (**See Column 3, Line 30 and Column 5, Lines 55-60**)

Shanklin fails to disclose calculating a hash value based on the data sufficient to identify the network connection with which the data packet is associated and *there is a static association between the hash value computed and the entities used to compute the hash value.*

Hooper discloses calculating a hash value based on the data sufficient to identify the network connection with which the data packet is associated. **(See Paragraphs 24 and 43. By definition after a hash value is computed it remains static and has a static relationship with the components used to compute the hash value. In this case, as long as the destination and source address used to compute the hash value do not change then the association between the computed hash value and the processors at the destination will not change and is therefore static. If the destination or source address used to compute the hash value changes then a new hash value has to be recomputed.)**

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Shanklin's system to incorporate hash value calculation based network connection data. The motivation being hash value calculation simplifies address lookup as stated in Hooper's Paragraph 24 and also saves processor time and provides additional level of security. Shanklin states in Column 3, Line 25 that his router uses the packet protocol level address to forward packets and Hooper in Paragraphs 24 and 43 elaborates how it is done using a hash value calculated based on the source and destination address.

Art Unit: 2616

6. Regarding **claim 2**, Shanklin discloses a method wherein the data in the data packet is sufficient to identify the network connection with which the data packet is associated comprises address data. **(See Column 3, Lines 25-26)**

7. Regarding **claim 3**, wherein the data sufficient to identify the network connection with which the data packet is associated comprises address data associated with a source computer that sent the data packet and address data associated with a destination computer to which the data packet is addressed. **(See Column 3, Lines 25-26, Column 4 Lines 12-15 and 25-30)**

8. Regarding **claim 4**, wherein the data packet is sent using the TCP/IP suite of protocols and the data sufficient to identify the network connection with which the data packet is associated comprises an IP address and port number associated with the source computer that sent the data packet and an IP address and port number associated with the destination computer to which the data packet is addressed. **(See Column 3, Lines 25-26, Column 4 Lines 12-15 and 25-30. Shanklin discloses the packets are sent using the TCP/IP protocol and the rest of the limitation is inherent to the protocol)**

9. Regarding **claim 5**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 1 but fails to disclose a method further comprising storing the data packet in host memory associated with the multi-processor system.

Hooper discloses a method further comprising storing the data packet in host memory associated with the multi-processor system. **(See Paragraph 14 and Figure 1)**

Art Unit: 2616

10. Regarding **claim 6**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 5 but fails to disclose a method, further comprising sending an interrupt message to a driver, the interrupt message comprising data identifying the storage location in host memory in which the data packet is stored.

Hooper discloses a method, further comprising sending an interrupt message to a driver, the interrupt message comprising data identifying the storage location in host memory in which the data packet is stored. **(See Paragraph 24)**

11. With respect to **claims 5 and 6**, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Shanklin's system to incorporate hash value calculation based network connection data and storing the data packet in host memory associated with the multi-processor system and sending an interrupt message. The motivation being these steps simplify address lookup as stated in Hooper's Paragraph 24 and also saves processor time and provides additional level of security.

12. Regarding **claim 7**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 1 but fails to disclose a method further comprising storing the data packet in host memory associated with the multi-processor system and wherein the step of routing comprises sending to the one of the plurality of processors data identifying the storage location in host memory in which the data packet is stored.

Hooper discloses a method further comprising storing the data packet in host memory associated with the multi-processor system and wherein the step of routing

Art Unit: 2616

comprises sending to the one of the plurality of processors data identifying the storage location in host memory in which the data packet is stored. **(See Paragraphs 13-15)**

13. Regarding **claim 8**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 7 but fails to disclose a method wherein the step of sending to the one of the plurality of processors data identifying the storage location in host system memory in which the data packet is stored comprises storing the data identifying the storage location in a work queue associated with the processor.

Hooper discloses a method wherein the step of sending to the one of the plurality of processors data identifying the storage location in host system memory in which the data packet is stored comprises storing the data identifying the storage location in a work queue associated with the processor. **(See Paragraph 21)**

14. Regarding **claim 9**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 8 but fails to disclose a method wherein the work queue is a circular queue.

Hooper discloses a method wherein the work queue is a circular queue. **(See Paragraph 21. Further as the Applicant readily admitted in the Specification on page 18, Line 12 that a circular work queue is well known to one ordinarily skilled in the art and hence Hooper's queue can easily be a circular work queue)**

15. With respect to **claims 7-9**, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Shanklin's system to incorporate hash value calculation based network connection data and storing the data packet in host memory associated with the multi-processor system and the step of

routing comprises sending to the one of the plurality of processors data identifying the storage location in a work queue in a host memory in which the data packet is stored.

The motivation being these steps simplify address lookup as stated in Hooper's Paragraph 24 and also saves processor time and provides additional level of security.

Hooper in Paragraph 13 states a further motivation in that it lends hand to low network latency and fast access.

16. Regarding **claim 10**, Shanklin discloses a method further comprising associating the data packet with one or more other data packets associated with the same network connection with which the received data packet is associated to recreate a network flow associated with the network connection. **(See Column 3, Lines 43-46)**

17. Regarding **claim 11**, Shanklin discloses a method further comprising analyzing the network flow to determine if any security-related event has occurred. **(See Column 3, Lines 55-65 and Column 5, Lines 30-40)**

18. Regarding **claim 12**, Shanklin discloses a method, wherein a security-related event is determined to have occurred if the network flow matches a pattern associated with a known attack. **(See Column 5, Lines 30-40, Column 6, Lines 4-8, and Column 7, Lines 60-65)**

19. Regarding **claim 13**, Shanklin discloses a method wherein a security-related event is determined to have occurred if the network flow deviates from normal and permissible behavior under the network protocol under which the data packet was sent. **(See Column 5, Lines 30-40, Column 6, Lines 4-8, and Column 7, Lines 60-65)**

Response to Arguments

20. Applicant's arguments filed 2/21/2006 have been fully considered but they are not persuasive.

21. In the Remarks, in the second paragraph on page 5, Applicant argues that the cited secondary reference, i.e. Hooper, teaches a hash table that can be dynamically modified and therefore fails to teach static association. Examiner respectfully disagrees with Applicant's conclusion.

By definition after a hash value is computed it remains static and has a static relationship with the components used to compute the hash value. In Hooper's case, as long as the destination and source address used to compute the hash value do not change then the association between the computed hash value and the processors at the destination will not change and is therefore static. If the destination or source address used to compute the hash value changes then a new hash value has to be recomputed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the

Art Unit: 2616

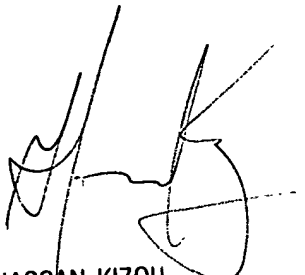
shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Habte Mered whose telephone number is 571 272 6046. The examiner can normally be reached on Monday to Friday 9:30AM to 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on 571 272 3088. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HM
05-03-2006



HASSAN KIZOU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600